CHAPTER

Domain 3: Security engineering

3

CHAPTER OUTLINE

Eleventh Hour CISSP®. http://dx.doi.org/10.1016/B978-0-12-811248-9.00003-6

INTRODUCTION

We begin this domain with security architecture concepts, including security models, as well as secure system components in hardware and software. Next comes cryptography, including core concepts of symmetric encryption, asymmetric encryption, and hash functions. Finally, we will discuss physical security, where we will learn that safety of personnel is paramount.

SECURITY MODELS

Security models provide rules of the road for security in operating systems. The canonical example is Bell-LaPadula, which includes "no read up" (NRU), also known as the Simple Security Property. This is the rule that forbids a secret-cleared subject from reading a top-secret object. While Bell-LaPadula, which is discussed shortly, is focused on protecting confidentiality, other models like Biba are focused on integrity.

READING DOWN AND WRITING UP

The concepts of reading down and writing up apply to mandatory access control models such as Bell-LaPadula. Reading down occurs when a subject reads an object at a lower sensitivity level, such as a top-secret subject reading a secret object.

There are instances when a subject has information and passes that information up to an object, which has higher sensitivity than the subject has permission to access. This is called writing up.

BELL-LAPADULA MODEL

The *Bell-LaPadula* model was originally developed for the US Department of defense (DoD). It is focused on maintaining the confidentiality of objects. Protecting confidentiality means users at a lower security level are denied access to objects at a higher security level.

FAST FACTS

Bell-LaPadula includes the following rules and properties:

- *Simple Security Property*: "No read up"; a subject at a specific clearance level cannot read an object at a higher classification level. Subjects with a Secret clearance cannot access Top Secret objects, for example.
- *Security Property*: "No write down"; a subject at a higher clearance level cannot write to a lower classification level. For example: subjects who are logged into a Top Secret system cannot send emails to a Secret system.
- *Strong Tranquility Property*: Security labels will not change while the system is operating.
- *Weak Tranquility Property*: Security labels will not change in a way that conflicts with defined security properties.

LATTICE-BASED ACCESS CONTROLS

Lattice-based access control allows security controls for complex environments. For every relationship between a subject and an object, there are defined upper and lower access limits implemented by the system. This lattice, which allows reaching higher and lower data classification, depends on the need of the subject, the label of the object, and the role the subject has been assigned. Subjects have a least upper bound (LUB) and greatest lower bound (GLB) of access to the objects based on their lattice position.

INTEGRITY MODELS

Models such as Bell-LaPadula focus on confidentiality, sometimes at the expense of integrity. The Bell-LaPadula "no write down" rule means subjects can write up; that is, a Secret subject can write to a Top Secret object. What if the Secret subject writes erroneous information to a Top Secret object? Integrity models such as Biba address this issue.

Biba model

While many governments are primarily concerned with confidentiality, most businesses desire to ensure that the integrity of the information is protected at the highest level. *Biba* is the model of choice when integrity protection is vital.

FAST FACTS

The Biba model has two primary rules: the Simple Integrity Axiom and the * Integrity Axiom.

- *Simple Integrity Axiom*: "No read down"; a subject at a specific clearance level cannot *read* data at a lower classification. This prevents subjects from accessing information at a lower integrity level. This protects integrity by preventing bad information from moving up from lower integrity levels.
- ** Integrity Axiom*: "No write up"; a subject at a specific clearance level cannot *write* data to a higher classification. This prevents subjects from passing information up to a higher integrity level than they have clearance to change. This protects integrity by preventing bad information from moving up to higher integrity levels.

Biba is often used where integrity is more important than confidentiality. Examples include time and location-based information.

DID YOU KNOW?

Biba takes the Bell-LaPadula rules and reverses them, showing how confidentiality and integrity are often at odds. If you understand Bell-LaPadula (no read up; no write down), you can extrapolate Biba by reversing the rules: "no read down"; "no write up."

Clark-Wilson

Clark-Wilson is a real-world integrity model that protects integrity by requiring subjects to access objects via programs. Because the programs have specific limitations to what they can and cannot do to objects, Clark-Wilson effectively limits the capabilities of the subject. Clark-Wilson uses two primary concepts to ensure that security policy is enforced: well-formed transactions and separation of duties. The concept of well-formed transactions provides integrity. The process is comprised of what is known as the access control triple: user, transformation procedure, and constrained data item.

CHINESE WALL MODEL

The Chinese Wall model (also known as Brewer-Nash) is designed to avoid conflicts of interest by prohibiting one person, such as a consultant, from accessing multiple conflict of interest categories (CoIs).

ACCESS CONTROL MATRIX

An access control matrix is a table that defines the access permissions that exist between specific subjects and objects. A matrix is a data structure that acts as a lookup table for the operating system. The table's rows, or capability lists, show the capabilities of each subject. The columns of the table show the access control list (ACL) for each object or application.

SECURE SYSTEM DESIGN CONCEPTS

Secure system design transcends specific hardware and software implementations and represents universal best practices.

LAYERING

Layering separates hardware and software functionality into modular tiers. The complexity of an issue, such as reading a sector from a disk drive, is contained to one layer; in this case, the hardware layer. One layer, such as the application layer, is not directly affected by a change to another.

FAST FACTS

A generic list of security architecture layers is as follows:

1. Hardware
2. *Kernel* and device drivers
3. *Operating system (OS)*
4. Applications

ABSTRACTION

Abstraction hides unnecessary details from the user. As Bruce Schneier said, "Complexity is the enemy of security"[1]; that is, the more complex a process, the less secure it is. That said, computers are tremendously complex machines, and abstraction provides a way to manage that complexity.

SECURITY DOMAINS

A *security domain* is the list of objects a subject is allowed to access. More broadly defined, domains are groups of subjects and objects with similar security requirements. Confidential, Secret, and Top Secret are three security domains used by the US DoD, for example.

THE RING MODEL

The *ring model* is a form of central processing unit (CPU) hardware layering that separates and protects domains, such as kernel mode and user mode, from each other. Many CPUs, such as the Intel x86 family, have four rings, ranging from Ring 0 (kernel) to Ring 3 (user), shown in Fig. 3.1. The innermost ring is the most trusted, and each successive outer ring is less trusted.

Processes communicate between the rings via *system calls*, which allow processes to communicate with the kernel and provide a window between the rings.

FAST FACTS

The rings are (theoretically) used as follows:

- *Ring 0*: Kernel
- *Ring 1*: Other OS components that do not fit into Ring 0
- *Ring 2*: Device drivers
- *Ring 3*: User applications

While x86 CPUs have four rings and can be used as described above, this usage is considered theoretical because most x86 operating systems, including Linux and Windows, use Rings 0 and 3 only. A new mode called hypervisor mode (and informally called "Ring −1") allows virtual guests to operate in Ring 0, controlled by the hypervisor one ring "below." The Intel Virtualization Technology (Intel VT, aka "Vanderpool"), and AMD-Virtualization (AMD-V, aka "Pacifica") CPUs support a hypervisor.

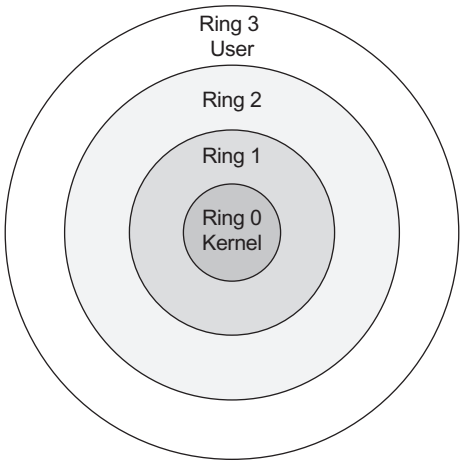

FIG. 3.1

The ring model.

OPEN AND CLOSED SYSTEMS

An *open system* uses open hardware and standards, using standard components from a variety of vendors. An IBM-compatible PC is an open system, using a standard motherboard, memory, BIOS, CPU, etc. You may build an IBM-compatible PC by purchasing components from a multitude of vendors. A *closed system* uses proprietary hardware or software.

DID YOU KNOW?

An open system is not the same as open source. An open system uses standard hardware and software, while open-source software makes source code publicly available.

SECURE HARDWARE ARCHITECTURE

Secure hardware architecture focuses on the physical computer hardware required to have a secure system. The hardware must provide confidentiality, integrity, and availability for processes, data, and users.

THE SYSTEM UNIT AND MOTHERBOARD

The *system unit* is the computer's case; it contains all of the internal electronic computer components, including the motherboard, internal disk drives, power supply, etc. The *motherboard* contains hardware including the CPU, memory slots, firmware, and peripheral slots, such as peripheral component interconnect slots. The keyboard unit is the external keyboard.

THE COMPUTER BUS

A *computer bus*, shown in Fig. 3.2, is the primary communication channel on a computer system. Communication between the CPU, memory, and input/output devices such as keyboard, mouse, and display occurs via the bus.

THE CPU

The central processing unit (CPU) is the brains of the computer, capable of controlling and performing mathematical calculations. Ultimately, everything a computer does is mathematical: adding numbers, which can be extended to subtraction, multiplication, division, etc.; performing logical operations; accessing memory locations by address; etc. CPUs are rated by the number of clock cycles per second. A 4-GHz CPU has four billion clock cycles per second.

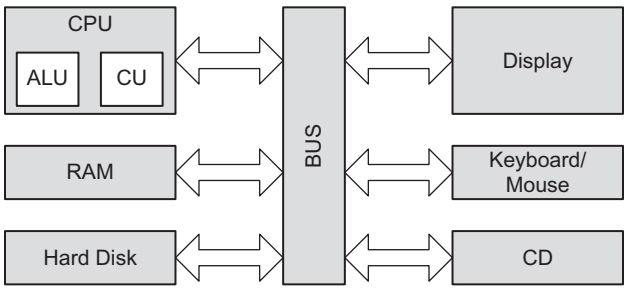

FIG. 3.2

Simplified computer bus.

Arithmetic logic unit and control unit

The *arithmetic logic unit* (ALU) performs mathematical calculations; it is the part that computes. The ALU is fed instructions by the *control unit*, which acts as a traffic cop, sending instructions to the ALU.

Fetch and execute

CPUs fetch machine language instructions (such as "add 1 + 1") and execute them (add the numbers, for answer of "2"). The "*fetch and execute*" (also called the fetch-decode-execute cycle or FDX) process actually takes four steps:

1. Fetch Instruction 1
2. Decode Instruction 1
3. Execute Instruction 1
4. Write (save) Result 1

These four steps take one clock cycle to complete.

Pipelining

Pipelining combines multiple CPU steps into one process, allowing simultaneous FDX and write steps for different instructions. Each part is called a pipeline stage; the pipeline depth is the number of simultaneous stages that may be completed at once.

Given our previous fetch-and-execute example of adding 1 + 1, a CPU without pipelining would have to wait an entire cycle before performing another computation. A four-stage pipeline can combine the stages of four other instructions:

1. Fetch Instruction 1
2. Fetch Instruction 2, Decode Instruction 1
3. Fetch Instruction 3, Decode Instruction 2, Execute Instruction 1
4. Fetch Instruction 4, Decode Instruction 3, Execute Instruction 2, Write (save) result 1
5. Fetch Instruction 5, Decode Instruction 4, Execute Instruction 3, Write (save) result 2, etc.

Pipelining is like an automobile assembly line; instead of building one car at a time, from start to finish, lots of cars enter the assembly pipeline, and discrete phases (like installing tires) occur on one car after another. This increases the throughput.

Interrupts

An *interrupt* indicates that an asynchronous event has occurred. A CPU interrupt is a form of hardware interrupt that causes the CPU to stop processing its current task, save the state, and begin processing a new request. When the new task is complete, the CPU will complete the prior task.

Processes and threads

A *process* is an executable program and its associated data loaded and running in memory. A heavyweight process (HWP) is also called a task. A parent process may spawn additional child processes called *threads*. A thread is a lightweight process (LWP). Threads are able to share memory, resulting in lower overhead compared to heavy weight processes.

Multitasking and multiprocessing

Applications run as processes in memory, comprised of executable code and data. *Multitasking* allows multiple tasks (heavyweight processes) to run simultaneously on one CPU. Older and simpler operating systems, such as MS-DOS, are non-multitasking, in that they run one process at a time. Most modern operating systems, such as Linux, Windows 10, and OS X support multitasking.

Multiprocessing has a fundamental difference from multitasking: it runs multiple processes on multiple CPUs. Two types of multiprocessing are symmetric multiprocessing (SMP) and asymmetric multiprocessing (AMP; some sources use ASMP). SMP systems have one operating system to manage all CPUs. AMP systems have one operating system image per CPU, essentially acting as independent systems.

CISC and RISC

CISC (complex instruction set computer) and RISC (reduced instruction set computer) are two forms of CPU design. CISC uses a large set of complex machine language instructions, while RISC uses a reduced set of simpler instructions. x86 CPUs, among many others, are CISC; ARM (used in many cell phones and PDAs), PowerPC, Sparc, and others are RISC.

MEMORY PROTECTION

Memory protection prevents one process from affecting the confidentiality, integrity, or availability of another. This is a requirement for secure multiuser (ie, more than one user logged in simultaneously) and multitasking (ie, more than one process running simultaneously) systems.

Process isolation

Process isolation is a logical control that attempts to prevent one process from interfering with another. This is a common feature among multiuser operating systems such as Linux, UNIX, or recent Microsoft Windows operating systems. Older operating systems such as MS-DOS provide no process isolation, which means a crash in any MS-DOS application could crash the entire system.

Hardware segmentation

Hardware segmentation takes process isolation one step further by mapping processes to specific memory locations. This provides more security than logical process isolation alone.

Virtual memory

Virtual memory provides virtual address mapping between applications and hardware memory. Virtual memory provides many functions, including multitasking (multiple tasks executing at once on one CPU), swapping, and allowing multiple processes to access the same shared library in memory, among others.

Swapping and paging

Swapping uses virtual memory to copy contents of primary memory (RAM) to or from secondary memory (not directly addressable by the CPU, on disk). Swap space is often a dedicated disk partition that is used to extend the amount of available memory. If the kernel attempts to access a page (a fixed-length block of memory) stored in swap space, a page fault occurs, which means that the page is not located in RAM and the page is "swapped" from disk to RAM.

Basic input/output system

The IBM PC-compatible basic input/output system (BIOS) contains code in firmware that is executed when a PC is powered on. It first runs the *power-on self-test* (POST), which performs basic tests, including verifying the integrity of the BIOS itself, testing the memory, and identifying system devices, among other tasks. Once the POST process is complete and successful, it locates the boot sector (for systems that boot off disks), which contains the machine code for the operating system kernel. The kernel then loads and executes, and the operating system boots up.

WORM storage

WORM (write once, read many) storage, like its name suggests, can be written to once and read many times. It is often used to support records retention for legal or regulatory compliance. WORM storage helps assure the integrity of the data it contains; there is some assurance that it has not been and cannot be altered, short of destroying the media itself.

TRUSTED PLATFORM MODULE

A trusted platform module (TPM) chip is a processor that can provide additional security capabilities at the hardware level. Not all computer manufacturers employ TPM chips, but the adoption has steadily increased. If included, a TPM chip is typically found on a system's motherboard.

The TPM chip allows for hardware-based cryptographic operations. Security functions can leverage the TPM for random number generation; the use of symmetric, asymmetric, and hashing algorithms; and secure storage of cryptographic keys and message digests. The most commonly referenced use case for the TPM chip is ensuring boot integrity. By operating at the hardware level, the TPM chip can help ensure that kernel-mode rootkits are less likely to be able to undermine operating system security. In addition to boot integrity, TPM is also commonly associated with some implementations of full disk encryption.

DATA EXECUTION PREVENTION AND ADDRESS SPACE LAYOUT RANDOMIZATION

One of the main goals in attempting to exploit software vulnerabilities is to achieve some form of code execution capability. The two most prominent protections against this attack are data execution prevention (DEP) and address space location randomization (ASLR). DEP, which can be enabled within hardware and/or software, attempts to prevent code execution in memory locations that are not predefined to contain executable content.

Another protection mechanism, ASLR, seeks to make exploitation more difficult by randomizing memory addresses. For example, imagine an adversary develops a successful working exploit on his or her own test machine. When the code is run on a different system using ASLR, the addresses will change, which will probably cause the exploit to fail.

SECURE OPERATING SYSTEM AND SOFTWARE ARCHITECTURE

Secure operating system and software architecture builds upon the secure hardware described in the previous section, providing a secure interface between hardware and the applications, as well as the users, that access the hardware. Operating systems provide memory, resource, and process management.

THE KERNEL

The kernel is the heart of the operating system, which usually runs in ring 0. It provides the interface between hardware and the rest of the operating system, including applications. As discussed previously, when an IBM-compatible PC is started or rebooted, the BIOS locates the boot sector of a storage device, such as a hard drive. That boot sector contains the beginning of the software kernel machine code, which is then executed.

Reference monitor

A core function of the kernel is running the *reference monitor*, which mediates all access between subjects and objects. It enforces the system's security policy, such as preventing a normal user from writing to a restricted file, like the system password file.

VIRTUALIZATION AND DISTRIBUTED COMPUTING

Virtualization and distributed computing have revolutionized the computing world, bringing wholesale changes to applications, services, systems data, and data centers.

VIRTUALIZATION

Virtualization adds a software layer between an operating system and the underlying computer hardware. This allows multiple "guest" operating systems to run simultaneously on one physical "host" computer.

Hypervisor

The key to virtualization security is the *hypervisor*, which controls access between virtual guests and host hardware. A Type 1 hypervisor, also called bare metal, is part of an operating system that runs directly on host hardware. A Type 2 hypervisor runs as an application on a normal operating system, such as Windows 10.

Many virtualization exploits target the hypervisor, including hypervisor-controlled resources shared between host and guests, or guest and guest. These include cut-and-paste, shared drives, and shared network connections.

Virtualization security issues

Virtualization software is complex and relatively new. As discussed previously, complexity is the enemy of security[1]; the sheer complexity of virtualization software may cause security problems.

Combining multiple guests onto one host may also raise security issues. Virtualization is no replacement for a firewall; never combine guests with different security requirements (such as DMZ and internal) onto one host. The risk of virtualization escape is called VMEscape, where an attacker exploits the host OS or a guest from another guest.

Many network-based security tools, such as network intrusion detection systems, can be blinded by virtualization.

CLOUD COMPUTING

Public cloud computing outsources IT infrastructure, storage, or applications to a third-party provider. A cloud also implies geographic diversity of computer resources. The goal of cloud computing is to allow large providers to leverage their economies of scale to provide computing resources to other companies that typically pay for these services based on their usage.

Table 3.1 Example Cloud Service Levels

Type	Example
Infrastructure as a Service (IaaS)	Linux server hosting
Platform as a Service (PaaS)	Web service hosting
Software as a Service (SaaS)	Web mail

Three commonly available levels of service provided by cloud providers are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). IaaS provides an entire virtualized operating system, which the customer configures from the OS on up. PaaS provides a preconfigured operating system and the customer configures the applications. Finally, SaaS is completely configured, from the operating system to applications, and the customer simply uses the application. In all three cases, the cloud provider manages hardware, virtualization software, network, backups, etc. See Table 3.1 for typical examples of each.

Private clouds house data for a single organization and may be operated by a third party or by the organization itself. Government clouds keep data and resources geographically contained within the borders of one country, designed for the government of the respective country.

Benefits of cloud computing include reduced upfront capital expenditure, reduced maintenance costs, robust levels of service, and overall operational cost savings.

From a security perspective, taking advantage of public cloud computing services requires strict service level agreements and an understanding of new sources of risk. One concern is that if multiple organizations' guests are running on the same host, the compromise of one cloud customer could lead to the compromise of other customers.

Organizations should also negotiate specific rights before signing a contract with a cloud computing provider. These rights include the right to audit, the right to conduct a vulnerability assessment, and the right to conduct a penetration test, both electronic and physical, of data and systems placed in the cloud.

GRID COMPUTING

Grid computing represents a distributed computing approach that attempts to achieve high computational performance by nontraditional means. Rather than achieving high-performance computational needs by having large clusters of similar computing resources or a single high-performance system, such as a supercomputer, grid computing attempts to harness the computational resources of a large number of dissimilar devices.

LARGE-SCALE PARALLEL DATA SYSTEMS

The primary purpose of large-scale parallel systems is to allow for increased performance through economies of scale. One of the key security concerns with parallel systems is ensuring the maintenance of data integrity throughout the processing.

Often parallel systems will leverage some degree of shared memory on which they operate. This shared memory, if not appropriately managed, can expose potential race conditions that introduce integrity challenges.

PEER-TO-PEER NETWORKS

Peer-to-peer (P2P) networks alter the classic client/server computer model. Any system may act as a client, a server, or both, depending on the data needs. Decentralized peer-to-peer networks are resilient; there are no central servers that can be taken offline.

Integrity is a key P2P concern. With no central repository of data, what assurance do users have of receiving legitimate data? Cryptographic hashes are a critical control and should be used to verify the integrity of data downloaded from a P2P network.

THIN CLIENTS

Thin clients are simpler than normal computer systems, which have hard drives, full operating systems, locally installed applications, etc. Thin clients rely on central servers, which serve applications and store the associated data. Thin clients allow centralization of applications and their data, as well as the associated security costs of upgrades, patching, data storage, etc. Thin clients may be hardware based (such as diskless workstations) or software based (such as thin client applications).

SYSTEM VULNERABILITIES, THREATS, AND COUNTERMEASURES

System threats, vulnerabilities, and countermeasures describe security architecture and design vulnerabilities, as well as the corresponding exploits that may compromise system security. We will also discuss countermeasures, or mitigating actions that reduce the associated risk.

COVERT CHANNELS

A *covert channel* is any communication that violates security policy. The communication channel used by malware installed on a system that locates personally identifiable information (PII) such as credit card information and sends it to a malicious server is an example of a covert channel. Two specific types of covert channels are *storage channels* and *timing channels*.

BACKDOORS

A *backdoor* is a shortcut in a system that allows a user to bypass security checks, such as username/password authentication, to log in. Attackers will often install a backdoor after compromising a system.

Maintenance hooks are a type of backdoor; they are shortcuts installed by system designers and programmers to allow developers to bypass normal system checks during development, such as requiring users to authenticate.

MALICIOUS CODE (MALWARE)

Malicious code or *malware* is the generic term for any type of software that attacks an application or system. There are many types of malicious code; viruses, worms, Trojans, and logic bombs can all cause damage to targeted systems. Zero-day exploits are malicious code (ie, a threat) for which there is no vendor-supplied patch, meaning there is an unpatched vulnerability.

Computer viruses

Computer viruses are malware that does not spread automatically; they require a host (such as a file) and a carrier to spread the virus from system to system (usually a human).

FAST FACTS

Types of viruses include:

- *Macro virus*: virus written in macro language (such as Microsoft Office or Microsoft Excel macros).
- *Boot sector virus*: virus that infects the boot sector of a PC, which ensures that the virus loads upon system startup.
- *Stealth virus*: a virus that hides itself from the OS and other protective software, such as antivirus software.
- *Polymorphic virus*: a virus that changes its signature upon infection of a new system, attempting to evade signature-based antivirus software.
- *Multipartite virus*: a virus that spreads via multiple vectors. Also called multipart virus.

Worms

Worms are malware that self-propagates (spreads independently). Worms typically cause damage two ways: first by the malicious code they carry and then the loss of network availability due to aggressive self-propagation.

Trojans

A Trojan (also called a Trojan horse) is malware that performs two functions: one benign, such as a game, and one malicious. The term derives from the Trojan horse described in Virgil's poem *The Aeneid*.

Rootkits

A rootkit is malware that replaces portions of the kernel and/or operating system. A user-mode rootkit operates in ring 3 on most systems, replacing operating system components in "userland." A kernel-mode rootkit replaces the kernel, or loads malicious loadable kernel modules. Kernel-mode rootkits operate in ring 0 on most operating systems.

Packers

Packers provide runtime compression of executables. The original executable is compressed, and a small decompresser is prepended to the executable. Upon execution, the decompresser unpacks the compressed executable machine code and runs it. Packers are a neutral technology that is used to shrink the size of executables. Many types of malware use packers, which can be used to evade signature-based malware detection.

Logic bombs

A *logic bomb* is a malicious program that is triggered when a logical condition is met, such as after a number of transactions have been processed, or on a specific date (also called a time bomb). Malware such as worms often contain logic bombs, behaving in one manner, then changing tactics on a specific date and time.

Antivirus software

Antivirus software is designed to prevent and detect malware infections. Signature-based antivirus software uses static signatures of known malware. Heuristic-based antivirus uses anomaly-based detection to attempt to identify behavioral characteristics of malware, such as altering the boot sector.

SERVER-SIDE ATTACKS

Server-side attacks (also called service-side attacks) are launched directly from an attacker (the client) to a listening service. Patching, system hardening, firewalls, and other forms of defense-in-depth mitigate server-side attacks. Organizations should not allow direct access to server ports from untrusted networks such as the Internet, unless the systems are hardened and placed on DMZ networks.

CLIENT-SIDE ATTACKS

Client-side attacks occur when a user downloads malicious content. The flow of data is reversed compared to server-side attacks: client-side attacks initiate from the victim who downloads content from the attacker.

Client-side attacks are difficult to mitigate for organizations that allow Internet access. Clients include word processing software, spreadsheets, media players, Web browsers, etc. Most firewalls are far more restrictive inbound compared to outbound; they were designed to "keep the bad guys out," and mitigate server-side attacks originating from untrusted networks. They often fail to prevent client-side attacks.

WEB ARCHITECTURE AND ATTACKS

The World Wide Web of 10 or more years ago was simpler. Most web pages were static, rendered in Hypertext Markup Language, or HTML. The advent of "Web 2.0," with dynamic content, multimedia, and user-created data has increased the attack surface of the Web, creating more attack vectors.

Applets

Applets are small pieces of mobile code that are embedded in other software such as web browsers. Unlike HTML, which provides a way to display content, applets are executables. The primary security concern is that applets are downloaded from servers, then run locally. Malicious applets may be able to compromise the security of the client.

Applets can be written in a variety of programming languages; two prominent applet languages are *Java* (by Oracle/Sun Microsystems) and *ActiveX* (by Microsoft). The term "applet" is used for Java and "control" for ActiveX, although they are functionally similar.

Java

Java is an object-oriented language used not only as a way to write applets, but also as a general-purpose programming language. Java platform-independent bytecode is interpreted by the Java Virtual Machine (JVM). The JVM is available for a variety of operating systems, including Linux, FreeBSD, and Microsoft Windows.

Java applets run in a sandbox, which segregates the code from the operating system. The sandbox is designed to prevent an attacker who is able to compromise a java applet from accessing system files, such as the password file.

ActiveX

ActiveX controls are the functional equivalent of Java applets. They use digital certificates instead of a sandbox to provide security. Unlike Java, ActiveX is a Microsoft technology that works on Microsoft Windows operating systems only.

Open web application security project

The Open Web Application Security Project (OWASP, see: http://www.owasp.org) represents one of the best application security resources. OWASP provides a tremendous number of free resources dedicated to improving organizations' application security posture. One of their best-known projects is the OWASP Top 10 project, which provides consensus guidance on what are considered to be the 10 most significant application security risks. The OWASP Top 10 is available at https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

In addition to the wealth of information about application security threats, vulnerabilities, and defenses, OWASP also maintains a number of security tools available for free download including a leading interception proxy called the Zed Attack Proxy (ZAP).

Extensible markup language

Extensible markup language, or XML, is a markup language designed as a standard way to encode documents and data. XML is similar to HTML, but it is more universal. XML is used on the web, but is not tied to it; XML can be used to store application configuration and output from auditing tools, among other things. Extensible means users may use XML to define their own data formats.

Service-oriented architecture

Service-oriented architecture (SOA) attempts to reduce application architecture down to a functional unit of a service. SOA is intended to allow multiple heterogeneous applications to be consumers of services. The service can be used and reused throughout an organization rather than built within each individual application that needs the functionality offered by the service.

Services are expected to be platform independent and able to be called in a generic way that is also independent of a particular programming language. The intent is that that any application may leverage the service simply by using standard means available within their programming language of choice. Services are typically published in some form of a directory that provides details about how the service can be used and what the service provides.

Though web services are not the only example, they are the most common example provided for the SOA model. XML or JavaScript Object Notation (JSON) is commonly used for the underlying data structures of web services. SOAP, originally an acronym for Simple Object Access Protocol, but now simply SOAP, or REST (Representational State Transfer) provides the connectivity, and the WSDL (Web Services Description Language) provides details about how the web services are to be invoked.

DATABASE SECURITY

Databases present unique security challenges. The sheer amount of data that may be housed in a database requires special security consideration. As we will see shortly in the "Inference and Aggregation" section, the logical connections database users may make by creating, viewing, and comparing records may lead to inference and aggregation attacks, requiring database security precautions such as *inference* controls and *polyinstantiation*.

Polyinstantiation

Polyinstantiation allows two different objects to have the same name. The word polyinstantiation is based on the Latin roots for multiple (poly) and instances (instantiation). Database polyinstantiation means two rows may have the same primary key, but different data.

Inference and aggregation

Inference and *aggregation* occur when a user is able to use lower-level access to learn restricted information. These issues occur in multiple realms, including database security.

Inference requires deduction. There is a mystery to be solved, and lower level details provide the clues. Aggregation is a mathematical process; a user asks every question, receives every answer, and derives restricted information.

Data mining

Data mining searches large amounts of data to determine patterns that would otherwise get "lost in the noise." Credit card issuers have become experts in data mining, searching millions of credit card transactions stored in their databases to discover

signs of fraud. Simple data mining rules, such as "X or more purchases, in Y time, in Z places" are useful in discovering stolen credit cards.

MOBILE DEVICE ATTACKS

A recent information security challenge is the number of mobile devices ranging from USB flash drives to laptops that are infected with malware outside of a security perimeter, then carried into an organization. Traditional network-based protection, such as firewalls and intrusion detection systems, are powerless to prevent the initial attack.

Mobile device defenses

Defenses include administrative controls such as restricting the use of mobile devices via policy. Technical controls to mitigate infected mobile computers include requiring authentication at OSI model Layer 2 via 802.1X. 802.1X authentication may be bundled with additional security functionality, such as verification of current patches and antivirus signatures.

Another mobile device security concern is the loss or theft of a mobile device, which threatens the confidentiality, integrity, and availability of the device and the data that resides on it. Backups can assure the availability and integrity of mobile data.

Full disk encryption (also known as whole disk encryption) ensures the confidentiality of mobile device data.

Remote wipe capability is another critical control, which describes the ability to erase and sometimes disable a mobile device that is lost or stolen.

CORNERSTONE CRYPTOGRAPHIC CONCEPTS

Cryptography is secret writing, a type of secure communication understood by the sender and intended recipient only. While it may be known that the data is being transmitted, the content of that data should remain unknown to third parties. Data in motion (moving on a network) and data at rest (stored on a device, such as a disk) may be encrypted for security.

KEY TERMS

Cryptology is the science of secure communications. *Cryptography* creates messages with hidden meaning; *cryptanalysis* is the science of breaking those encrypted messages to recover their meaning. Many use the term cryptography in place of cryptology; however, it is important to remember that cryptology encompasses both cryptography and cryptanalysis.

A *cipher* is a cryptographic algorithm. A *plaintext* is an unencrypted message. *Encryption* converts a plaintext to a *ciphertext*. *Decryption* turns a ciphertext back into a plaintext.

CONFIDENTIALITY, INTEGRITY, AUTHENTICATION, AND NONREPUDIATION

Cryptography can provide confidentiality (secrets remain secret) and integrity (data is not altered without authorization). It is important to note that it does not directly provide availability. Cryptography can also provide authentication, which proves an identity claim.

Additionally, cryptography can provide *nonrepudiation*, which is an assurance that a specific user performed a specific transaction that did not change.

CONFUSION, DIFFUSION, SUBSTITUTION, AND PERMUTATION

Diffusion means the order of the plaintext should be "diffused" or dispersed in the ciphertext. *Confusion* means that the relationship between the plaintext and ciphertext should be as confused or random as possible.

Cryptographic *substitution* replaces one character for another; this provides the confusion. *Permutation*, also called transposition, provides diffusion by rearranging the characters of the plaintext, anagram-style. For example, "ATTACKATDAWN" can be rearranged to "CAAKDTANTATW."

DID YOU KNOW?

Strong encryption destroys patterns. If a single bit of plaintext changes, the odds of every bit of resulting ciphertext changing should be 50/50. Any signs of nonrandomness can be clues for a cryptanalyst, hinting at the underlying order of the original plaintext or key.

CRYPTOGRAPHIC STRENGTH

Good encryption is strong. For key-based encryption, it should be very difficult (ideally, impossible) to convert a ciphertext back to a plaintext without the key. The *work factor* describes how long it will take to break a cryptosystem (decrypt a ciphertext without the key).

Secrecy of the cryptographic algorithm does not provide strength; in fact, secret algorithms are often proven quite weak. Strong crypto relies on math, not secrecy, to provide strength. Ciphers that have stood the test of time are public algorithms, such as the *Triple Data Encryption Standard* (TDES) and the Advanced Encryption Standard (AES).

MONOALPHABETIC AND POLYALPHABETIC CIPHERS

A *monoalphabetic cipher* uses one alphabet, in which a specific letter substitutes for another. A *polyalphabetic cipher* uses multiple alphabets; for example, E substitutes for X one round, then S the next round.

Monoalphabetic ciphers are susceptible to frequency analysis. Polyalphabetic ciphers attempt to address this issue via the use of multiple alphabets.

EXCLUSIVE OR

Exclusive OR (XOR) is the "secret sauce" behind modern encryption. Combining a key with a plaintext via XOR creates a ciphertext. XORing the same key to the ciphertext restores the original plaintext. XOR math is fast and simple, so simple that it can be implemented with phone relay switches.

Two bits are true (or 1) if one or the other (exclusively, not both) is 1. In other words: if two bits are different, the answer is 1 (true). If two bits are the same, the answer is 0 (false). XOR uses a *truth table*, shown in Table 3.2. This dictates how to combine the bits of a key and plaintext.

DATA AT REST AND DATA IN MOTION

Cryptography protects data at rest and data in motion, or data in transit. Full disk encryption (also called whole disk encryption) of a magnetic disk drive using software such as BitLocker or PGP Whole Disk Encryption is an example of encrypting data at rest. An SSL or IPsec VPN is an example of encrypting data in motion.

PROTOCOL GOVERNANCE

Cryptographic *protocol governance* describes the process of selecting the right method (ie, cipher) and implementation for the right job, typically on an organization-wide scale. For example, as we will learn later this chapter, a digital signature provides authentication and integrity, but not confidentiality. Symmetric ciphers are primarily used for confidentiality, and AES is preferable over DES due to its strength and performance.

TYPES OF CRYPTOGRAPHY

There are three primary types of modern encryption: *symmetric*, *asymmetric*, and *hashing*. Symmetric cryptography uses a single key to encrypt and decrypt. Asymmetric cryptography uses two keys, one to encrypt and the other to decrypt. Hashing is a one-way cryptographic transformation using an algorithm, but no key.

Table 3.2 XOR Truth Table

X	*Y*	*X* XOR *Y*
0	0	0
0	1	1
1	0	1
1	1	0

SYMMETRIC ENCRYPTION

Symmetric encryption uses a single key to encrypt and decrypt. If you encrypt a zip file, then decrypt with the same key, you are using symmetric encryption. Symmetric encryption is also called "secret key" encryption because the key must be kept secret from third parties. Strengths of this method include speed and cryptographic strength per bit of key; however, the major weakness is that the key must be securely shared before two parties may communicate securely.

Stream and block ciphers

Symmetric encryption may have stream and block modes. Stream mode means each bit is independently encrypted in a "stream." Block mode ciphers encrypt blocks of data each round; for example, 64 bits for the Data Encryption Standard (DES), and 128 bits for AES. Some block ciphers can emulate stream ciphers by setting the block size to 1 bit; they are still considered block ciphers.

Initialization vectors and chaining

Some symmetric ciphers use an initialization vector to ensure that the first encrypted block of data is random. This ensures that identical plaintexts encrypt to different ciphertexts. Also, as Bruce Schneier notes in *Applied Cryptography*, "Even worse, two messages that begin the same will encrypt the same way up to the first difference. Some messages have a common header: a letterhead, or a 'From' line, or whatever."[2] Initialization vectors solve this problem.

Chaining (called *feedback* in stream modes) seeds the previous encrypted block into the next block ready for encryption. This destroys patterns in the resulting ciphertext. DES *Electronic Code Book* mode (see below) does not use an initialization vector or chaining, and patterns can be clearly visible in the resulting ciphertext.

DES

DES is the data encryption standard, which describes the *data encryption algorithm* (DEA). IBM designed DES, based on their older Lucifer symmetric cipher, which uses a 64-bit block size (ie, it encrypts 64 bits each round) and a 56-bit key.

EXAM WARNING

Even though DES is commonly referred to as an algorithm, it is technically the name of the published standard that describes DEA. It may sound like splitting hairs, but that is an important distinction to keep in mind on the exam. DEA may be the best answer for a question regarding the algorithm itself.

Modes of DES

DES can use five different modes to encrypt data. The modes' primary difference is block versus emulated stream, the use of initialization vectors, and whether errors in encryption will propagate to subsequent blocks.

FAST FACTS

The five modes of DES are:

- Electronic Code Book (ECB)
- Cipher Block Chaining (CBC)
- Cipher Feedback (CFB)
- Output Feedback (OFB)
- Counter (CTR) Mode

ECB is the original mode of DES. CBC, CFB, and OFB were added later. CTR mode is the newest mode, described in *NIST Special Publication 800-38a* (see http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf).

Electronic code book

ECB is the simplest and weakest form of DES. It uses no initialization vector or chaining. Identical plaintexts with identical keys encrypt to identical ciphertexts. Two plaintexts with partial identical portions, such as the header of a letter, encrypted with the same key will have partial identical ciphertext portions.

Cipher block chaining

CBC mode is a block mode of DES that XORs the previous encrypted block of ciphertext to the next block of plaintext to be encrypted. The first encrypted block is an initialization vector that contains random data. This "chaining" destroys patterns. One limitation of the CBC mode is that encryption errors will propagate; an encryption error in one block will cascade through subsequent blocks due to the chaining, therefore destroying their integrity.

Cipher feedback

CFB mode is very similar to CBC, but the primary difference is that CFB is a stream mode. It uses feedback, which is the name for chaining when used in stream modes, to destroy patterns. Like CBC, CFB uses an initialization vector and destroys patterns, and so errors propagate.

Output feedback

OFB mode differs from CFB in the way feedback is accomplished. CFB uses the previous ciphertext for feedback. The previous ciphertext is the subkey XORed to the plaintext. OFB uses the subkey *before* it is XORed to the plaintext. Since the subkey is not affected by encryption errors, errors will not propagate.

Counter

CTR mode is like OFB; the difference again is the feedback. CTR mode uses a counter, so this mode shares the same advantages as OFB in that patterns are destroyed and errors do not propagate. However, there is an additional advantage: since the feedback can be as simple as an ascending number, CTR mode encryption can be executed in parallel.

Table 3.3 summarizes the five modes of DES.

Table 3.3 Modes of DES Summary

	Type	Initialization Vector	Error Propagation?
Electronic code book (ECB)	Block	No	No
Cipher block chaining (CBC)	Block	Yes	Yes
Cipher feedback (CFB)	Stream	Yes	Yes
Output feedback (OFB)	Stream	Yes	No
Counter mode (CTR)	Stream	Yes	No

Single DES

Single DES is the original implementation of DES, encrypting 64-bit blocks of data with a 56-bit key, using 16 rounds of encryption. The work factor required to break DES was reasonable in 1976, but advances in CPU speed and parallel architecture have made DES weak to a *brute-force* key attack today, where every possible key is generated and attempted.

Triple DES

Triple DES applies single DES encryption three times per block. Formally called the "triple data encryption algorithm (TDEA) and commonly called TDES," it became a recommended standard in 1999.

International data encryption algorithm

The international data encryption algorithm (IDEA) is a symmetric block cipher designed as an international replacement to DES. It uses a 128-bit key and 64-bit block size. The IDEA has patents in many countries.

Advanced encryption standard

The advanced encryption standard (AES) is the current US standard in symmetric block ciphers. AES uses 128-bit (with 10 rounds of encryption), 192-bit (with 12 rounds of encryption), or 256-bit (with 14 rounds of encryption) keys to encrypt 128-bit blocks of data.

Choosing AES

The US National Institute of Standards and Technology (NIST) solicited input on a replacement for DES in the *Federal Register* in January 1997. Fifteen AES candidates were announced in August 1998, and the list was reduced to five in August 1999. Table 3.4 lists the five AES finalists.

Rijndael was chosen and became AES. AES has four functions: SubBytes, ShiftRows, MixColumns, and AddRoundKey.

Blowfish and Twofish

Blowfish and Twofish are symmetric block ciphers created by teams lead by Bruce Schneier, author of *Applied Cryptography*. Blowfish uses from 32- through 448-bit keys (the default is 128-bit) to encrypt 64 bits of data. Twofish was an AES finalist,

Table 3.4 Five AES Finalists

Name	Author
MARS	IBM (11 authors)
RC6	RSA (Rivest, Robshaw, Sidney, Yin)
Rijndael	Daemen, Rijmen
Serpent	Anderson, Biham, Knudsen
Twofish	Schneier, Kelsey, Hall, Ferguson, Whiting, Wagner

encrypting 128-bit blocks using 128-bit through 256-bit keys. Both are open algorithms, meaning they are unpatented and freely available.

RC5 and RC6

RC5 and RC6 are symmetric block ciphers by RSA Laboratories. RC5 uses 32-bit (testing purposes), 64-bit (replacement for DES), or 128-bit blocks. The key size ranges from zero to 2040 bits.

RC6 was an AES finalist. RC6 is based on RC5 and is altered to meet the AES requirements. It is also stronger than RC5, encrypting 128-bit blocks using 128-, 192-, or 256-bit keys.

ASYMMETRIC ENCRYPTION

Asymmetric encryption uses two keys, one for encryption and the other for decryption. The public key, as its name indicates, is made public, and asymmetric encryption is also called public key encryption for this reason. Anyone who wants to communicate with you may simply download your posted public key and use it to encrypt their plaintext. Once encrypted, your public key cannot decrypt the plaintext, but your *private key* can do so. As the name implies, your private key must be kept private and secure.

Additionally, any message encrypted with the private key may be decrypted with the public key, as it is for digital signatures, as we will see shortly.

Asymmetric methods

Math lies behind the asymmetric breakthrough. These methods use one-way functions, which are easy to compute one way but are difficult to compute in the reverse direction.

Factoring prime numbers

An example of a one-way function is factoring a composite number into its primes. Multiplying the prime number 6269 by the prime number 7883 results in the composite number 49,418,527. That way is quite easy to compute, as it takes just milliseconds on a calculator. However, answering the question "Which prime number times which prime number equals 49,418,527" is *much* more difficult.

That computation is called factoring, and no shortcut has been found for hundreds of years. Factoring is the basis of the RSA algorithm.

Discrete logarithm

A logarithm is the opposite of exponentiation. Computing 7 to the 13th power (exponentiation) is easy on a modern calculator: 96,889,010,407. Asking the question "96,889,010,407 is 7 to what power," which means to find the logarithm, is more difficult. Discrete logarithms apply logarithms to groups, which is a much harder problem to solve. This one-way function is the basis of the *Diffie-Hellman* and *ElGamal* asymmetric algorithms.

Diffie-Hellman key agreement protocol

Key agreement allows two parties the security with which to agree on a symmetric key via a public channel, such as the Internet, with no prior key exchange. An attacker who is able to sniff the entire conversation is unable to derive the exchanged key. Whitfield Diffie and Martin Hellman created the Diffie-Hellman Key Agreement Protocol (also called the Diffie-Hellman Key Exchange) in 1976. Diffie-Hellman uses discrete logarithms to provide security.

Elliptic curve cryptography

ECC leverages a one-way function that uses discrete logarithms as applied to elliptic curves. Solving this problem is harder than solving discrete logarithms, so algorithms based on elliptic curve cryptography (ECC) are much stronger per bit than systems using discrete logarithms (and also stronger than factoring prime numbers). ECC requires less computational resources because it uses shorter keys comparison to other asymmetric methods. Lower-power devices often use ECC for this reason.

Asymmetric and symmetric tradeoffs

Asymmetric encryption is far slower than symmetric encryption, and it is weaker per bit of key length. The strength of asymmetric encryption is the ability to communicate securely without presharing a key.

HASH FUNCTIONS

A hash function provides encryption using an algorithm and no key. They are called one-way hash functions because there is no way to reverse the encryption. A variable-length plaintext is "hashed" into a fixed-length hash value, which is often called a "message digest" or simply a "hash." Hash functions are primarily used to provide integrity: if the hash of a plaintext changes, the plaintext itself has changed. Common older hash functions include *secure hash algorithm 1* (SHA-1), which creates a 160-bit hash and *Message Digest 5* (MD5), which creates a 128-bit hash. There are weaknesses in both MD5 and SHA-1, so newer alternatives such as SHA-2 are recommended.

Collisions

Hashes are not unique because the number of possible plaintexts is far larger than the number of possible hashes. Assume you are hashing documents that are a megabit long with MD5. Think of the documents as strings that are 1,000,000 bits long, and think of the MD5 hash as a string 128 bits long. The universe of potential 1,000,000-bit strings is clearly larger than the universe of 128-bit strings. Therefore, more than one document could have the same hash' this is called a *collision*.

MD5

MD5 is the Message Digest algorithm 5. It is the most widely used of the MD family of hash algorithms. MD5 creates a 128-bit hash value based on any input length. MD5 has been quite popular over the years, but there are weaknesses where collisions can be found in a more practical amount of time. MD6 is the newest version of the MD family of hash algorithms, first published in 2008.

Secure hash algorithm

Secure hash algorithm (SHA) is the name of a series of hash algorithms. SHA-1 creates a 160-bit hash value. SHA-2 includes SHA-224, SHA-256, SHA-384, and SHA-512, named after the length of the message digest each creates.

CRYPTOGRAPHIC ATTACKS

Cryptanalysts use cryptographic attacks to recover the plaintext without the key. Please remember that recovering the key (which is sometimes called "stealing" the key) is usually easier than breaking modern encryption. This is what law enforcement officials typically do when tracking a suspect who used cryptography; they obtain a search warrant and attempt to recover the key.

BRUTE FORCE

A brute-force attack generates the entire key space, which is every possible key. Given enough time, the plaintext will be recovered.

SOCIAL ENGINEERING

Social engineering uses the human mind to bypass security controls. This technique may recover a key by tricking the key holder into revealing the key. Techniques are varied; one way is to impersonate an authorized user when calling a help desk to request a password reset.

KNOWN PLAINTEXT

A known plaintext attack relies on recovering and analyzing a matching plaintext and ciphertext pair; the goal is to derive the key that was used. You may be wondering why you would need the key if you already have the plaintext, but recovering the key would allow you to also decrypt other ciphertexts encrypted with the same key.

CHOSEN PLAINTEXT AND ADAPTIVE CHOSEN PLAINTEXT

A cryptanalyst chooses the plaintext to be encrypted in a chosen plaintext attack; the goal is to derive the key. Encrypting without knowing the key is accomplished via an encryption oracle, or a device that encrypts without revealing the key.

Adaptive-chosen plaintext begins with a chosen plaintext attack in the first round. The cryptanalyst then "adapts" further rounds of encryption based on the previous round.

CHOSEN CIPHERTEXT AND ADAPTIVE CHOSEN CIPHERTEXT

Chosen ciphertext attacks mirror chosen plaintext attacks; the difference is that the cryptanalyst chooses the ciphertext to be decrypted. This attack is usually launched against asymmetric cryptosystems, where the cryptanalyst may choose public documents to decrypt that are signed (encrypted) with a user's private key.

Adaptive-chosen ciphertext also mirrors its plaintext cousin: it begins with a chosen ciphertext attack in the first round. The cryptanalyst then adapts further rounds of decryption based on the previous round.

KNOWN KEY

The term "known-key attack" is misleading, because if the cryptanalyst knows the key, the attack is over. Known key means the cryptanalyst knows something about the key and can use that knowledge to reduce the efforts used to attack it. If the cryptanalyst knows that the key is an uppercase letter and a number only, other characters can be omitted in the attack.

DIFFERENTIAL CRYPTANALYSIS

Differential cryptanalysis seeks to find the difference between related plaintexts that are encrypted. The plaintexts may differ by a few bits. It launches as an adaptive chosen plaintext attack; the attacker chooses the plaintext to be encrypted though he or she does not know the key and then encrypts related plaintexts.

LINEAR CRYPTANALYSIS

Linear cryptanalysis is a known plaintext attack where the cryptanalyst finds large amounts of plaintext/ciphertext pairs created with the same key. The pairs are studied to derive information about the key used to create them.

Both differential and linear analysis can be combined as *differential linear analysis*.

SIDE-CHANNEL ATTACKS

Side-channel attacks use physical data to break a cryptosystem, such as monitoring CPU cycles or power consumption used while encrypting or decrypting.

IMPLEMENTING CRYPTOGRAPHY

Symmetric, asymmetric, and hash-based cryptography do not exist in a vacuum; rather, they have real-world applications, often in combination with each other, in which they can provide confidentiality, integrity, authentication, and nonrepudiation.

DIGITAL SIGNATURES

Digital signatures are used to cryptographically sign documents. Digital signatures provide nonrepudiation, which includes authentication of the identity of the signer, and proof of the document's integrity (proving the document did not change). This means the sender cannot later deny or repudiate signing the document.

Roy wants to send a digitally signed email to Rick. Roy writes the email, which is the plaintext. He then uses the SHA-1 hash function to generate a hash value of the plaintext. He then creates the digital signature by encrypting the hash with his RSA private key. Fig. 3.3 shows this process. Roy then attaches the signature to his plaintext email and hits send.

Rick receives Roy's email and generates his own SHA-1 hash value of the plaintext email. Rick then decrypts the digital signature with Roy's RSA public key, recovering the SHA-1 hash Roy generated. Rick then compares his SHA-1 hash with Roy's. Fig. 3.4 shows this process.

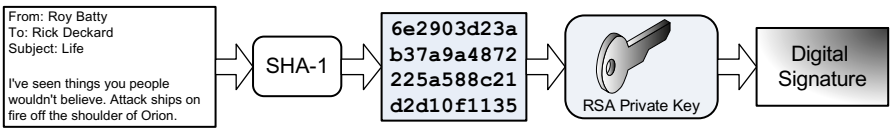

FIG. 3.3

Creating a digital signature[3].

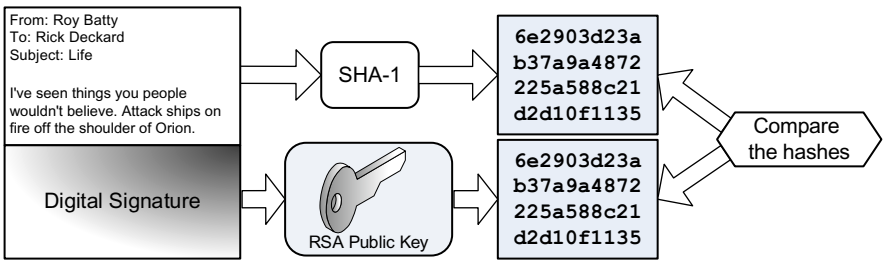

FIG. 3.4

Verifying a digital signature.

If the two hashes match, Rick knows a number of things:

1. Roy must have sent the email (only Roy knows his private key). This authenticates Roy as the sender.
2. The email did not change. This proves the integrity of the email.

If the hashes match, Roy cannot later deny having signed the email. This is nonrepudiation. If the hashes do not match, Rick knows either Roy did not send it, or that the email's integrity was violated.

PUBLIC KEY INFRASTRUCTURE

Public Key Infrastructure (PKI) leverages all three forms of encryption to provide and manage *digital certificates*. A digital certificate is a public key signed with a digital signature. Digital certificates may be server-based or client-based. If client and server certificates are used together, they provide mutual authentication and encryption. The standard digital certificate format is X.509.

Certificate authorities and organizational registration authorities

Digital certificates are issued by *certificate authorities* (CAs). Organizational registration authorities (ORAs) authenticate the identity of a certificate holder before issuing a certificate to them. An organization may operate as a CA or ORA (or both).

Certificate revocation lists

The CAs maintain *certificate revocation lists* (CRL), which, as the name implies, is a list of revoked certificates. A certificate may be revoked if the private key has been stolen, an employee is terminated, etc. A CRL is a flat file and does not scale well. The *Online Certificate Status Protocol* (OCSP) is a replacement for CRLs and uses client-server design that scales better.

Key management issues

CAs issue digital certificates and distribute them to certificate holders. The confidentiality and integrity of the holder's private key must be assured during the distribution process.

Public/private key pairs used in PKI should be stored centrally and securely. Users may lose their private key as easily as they may forget their password. A lost private key means that anything encrypted with the matching public key will be lost, short of cryptanalysis, as described previously.

Note that key storage is different than key escrow. Key storage means the organization that issued the public/private key pairs retains a copy. Key escrow means a copy is retained by a third-party organization (and sometimes multiple organizations), often for law enforcement purposes.

A retired key may not be used for new transactions, but one may be used to decrypt previously encrypted plaintexts. A destroyed key no longer exists and therefore cannot be used for any purpose.

SSL AND TLS

Secure Sockets Layer (SSL) brought the power of PKI to the web. SSL authenticates and provides confidentiality to web traffic. *Transport Layer Security* (TLS) is the successor to SSL. Both are commonly used as part of HTTPS (*Hypertext Transfer Protocol Secure*).

SSL was developed for the Netscape Web browser in the 1990s. SSL 2.0 was the first released version; SSL 3.0 fixed a number of security issues with version 2. TLS was based on SSL 3.0. TLS is very similar to that version, with some security improvements. Although typically used for HTTPS to secure web traffic, TLS may be used for other applications, such as Internet chat and email access.

IPsec

Internet Protocol Security (IPsec) is a suite of protocols that provide a cryptographic layer to both IPv4 and IPv6. It is one of the methods used to provide *virtual private networks* (VPN), which allow you to send private data over an insecure network, such as the Internet; the data crosses a public network, but is "virtually private." IPsec includes two primary protocols: *Authentication Header* (AH) and *Encapsulating Security Payload* (ESP). AH and ESP provide different and sometimes overlapping functionality.

Supporting IPsec protocols include *Internet Security Association and Key Management Protocol* (ISAKMP) and *Internet Key Exchange* (IKE).

AH and ESP

Authentication header (AH) provides authentication and integrity for each packet of network data. AH provides no confidentiality; it acts as a digital signature for the data. AH also protects against *replay attacks,* where data is sniffed off a network and resent, often in an attempt to fraudulently reuse encrypted authentication credentials.

ESP primarily provides confidentiality by encrypting packet data. It may also optionally provide authentication and integrity.

Security association and ISAKMP

AH and ESP may be used separately or in combination. An IPsec Security Association (SA) is a simplex (one-way) connection that may be used to negotiate ESP or AH parameters. If two systems communicate via ESP, they use two SAs, one for each direction. If the systems leverage AH in addition to ESP, they use two more SAs for a total of four. A unique 32-bit number called the security parameter index (SPI) identifies each simplex SA connection. The internet security association and key management protocol (ISAKMP) manages the SA creation process.

Tunnel and transport mode

IPsec is used in tunnel mode or transport mode. Security gateways use tunnel mode because they can provide point-to-point IPsec tunnels. ESP tunnel mode encrypts the entire packet, including the original packet headers. ESP transport mode only encrypts the data, not the original headers; this is commonly used when the sending and receiving system can "speak" IPsec natively.

CRUNCH TIME

AH authenticates the original IP headers, so it is often used (along with ESP) in transport mode because the original headers are not encrypted. Tunnel mode typically uses ESP alone, as the original headers are encrypted and thus protected by ESP).

IKE

IPsec can use a variety of encryption algorithms, such as MD5 or SHA-1 for integrity, and Triple DES or AES for confidentiality. The IKE negotiates the algorithm selection process. Two sides of an IPsec tunnel will typically use IKE to negotiate to the highest and fastest level of security, selecting AES over single DES for confidentiality if both sides support AES, for example.

PGP

Pretty Good Privacy (PGP), created by Phil Zimmerman in 1991, brought asymmetric encryption to the masses. PGP provides the modern suite of cryptography: confidentiality, integrity, authentication, and nonrepudiation. PGP can encrypt emails, documents, or an entire disk drive. PGP uses a *web of trust* model to authenticate digital certificates, instead of relying on a central CA.

S/MIME

MIME (multipurpose Internet mail extensions) provides a standard way to format email, including characters, sets, and attachments. Secure MIME (S/MIME) leverages PKI to encrypt and authenticate MIME-encoded email. The client or client's email server, called an S/MIME gateway, may perform the encryption.

ESCROWED ENCRYPTION

Escrowed encryption means a third-party organization holds a copy of a public/private key pair. The private key is often divided into two or more parts, each held in escrow by different trusted third-party organizations, which will only release their portion of the key with proper authorization, such as a court order. This provides separation of duties.

PERIMETER DEFENSES

Perimeter defenses help prevent, detect, and correct unauthorized physical access. Buildings, like networks, should employ defense in depth. Any one defense can fail, so critical assets should be protected by multiple physical security controls, such as fences, doors, walls, locks, etc. The ideal perimeter defense is safe, prevents unauthorized ingress, and offers both authentication and accountability, when applicable.

FENCES

Fences may range from simple deterrents (such as 3-foot/1-m tall fencing) to preventive devices, such as an 8-foot-tall (2.4 m) fence with barbed wire on top. Fences should be designed to steer ingress and egress to controlled points, such as exterior doors and gates.

GATES

Gates range in strength from Class 1, an ornamental gate designed to deter access, to a Class IV gate designed to prevent a car from crashing through entrances at airports and prisons.

FAST FACTS

Here are the four classes of gates:

- *Class I*: Residential (home use)
- *Class II*: Commercial/General Access (parking garage)
- *Class III*: Industrial/Limited Access (loading dock for 18-wheeler trucks)
- *Class IV*: Restricted Access (airport or prison)

LIGHTS

Lights can act as both a detective and deterrent control. A light that allows a guard to see an intruder is acting as a detective control. Types of lights include Fresnel lights, named after Augustine-Jean Fresnel. These are the same type of lights originally used in lighthouses, which used Fresnel lenses to aim light in a specific direction.

Light measurement terms include *lumen*, which is the amount of light one candle creates. Historically, light was measured in *foot-candles*, with one foot-candle measuring one lumen per square foot. *Lux*, based on the metric system, is more commonly used now; one lux is one lumen per square meter.

CCTV

Closed-circuit television (CCTV) is a detective device used to aid guards in detecting the presence of intruders in restricted areas. CCTVs using the normal light spectrum require sufficient visibility to illuminate the field of view that is visible to the camera. Infrared devices can "see in the dark" by displaying heat. Older "tube cameras" are analog devices. Modern cameras use charge-coupled discharge (CCD), which is digital.

Cameras have mechanical irises that act as human irises, controlling the amount of light that enters the lens by changing the size of the aperture. Key issues include *depth of field*, which is the area that is in focus, and *field of view*, which is the entire area viewed by the camera. More light allows a larger depth of field because a smaller aperture places more of the image in focus. Correspondingly, a wide aperture (used in lower light conditions) lowers the depth of field.

CCTV cameras may also have other typical camera features such as pan and tilt (moving horizontally and vertically).

LOCKS

Locks are a preventive physical security control, used on doors and windows to prevent unauthorized physical access. Locks may be mechanical, such as key locks or combination locks, while electronic locks are often used with smart cards or magnetic stripe cards.

Key locks

Key locks require a physical key to unlock. Keys are shared or sometimes copied, which lowers the accountability of key locks. A common type is the pin tumbler lock, which has driver pins and key pins. The correct key makes the pins line up with the shear line, allowing the lock tumbler (plug) to turn.

Ward or *warded locks* must turn a key through channels, or wards. A skeleton key can open varieties of warded locks.

Combination locks

Combination locks have dials that must be turned to specific numbers in a specific order (ie, alternating clockwise and counterclockwise turns) to unlock. Button or keypad locks also use numeric combinations. Limited accountability due to shared combinations is the primary security issue concerning these types of locks.

SMART CARDS AND MAGNETIC STRIPE CARDS

A *smart card* is a physical access control device that is often used for electronic locks, credit card purchases, or dual-factor authentication systems. "Smart" means the card contains a computer circuit; another term for a smart card is *integrated circuit card* (ICC).

Smart cards may be "contact" or "contactless." Contact cards use a smart card reader, while contactless cards are read wirelessly. One type of contactless card technology is *radio-frequency identification* (RFID). These cards contain RFID tags (also called transponders) that are read by RFID transceivers.

A *magnetic stripe* card contains a magnetic stripe that stores information. Unlike smart cards, magnetic stripe cards are passive devices that contain no circuits. These cards are sometimes called swipe cards because they are read when swiped through a card reader.

TAILGATING/PIGGYBACKING

Tailgating, also known as *piggybacking*, occurs when an unauthorized person follows an authorized person into a building after the authorized person unlocks and opens the door. Policy should forbid employees from allowing tailgating and security awareness efforts should describe this risk.

MANTRAPS AND TURNSTILES

A *mantrap* is a preventive physical control with two doors. The first door must close and lock before the second door may be opened. Each door typically requires a separate form of authentication to open, such as biometrics or a personal identification number (PIN). Without authentication, the intruder is trapped between the doors after entering the mantrap.

Turnstiles are designed to prevent tailgating by enforcing a "one person per authentication" rule, just as they do in subway systems. Secure data centers often use floor-to-ceiling turnstiles with interlocking blades to prevent an attacker from going over or under the turnstile. Secure revolving doors perform the same function.

CONTRABAND CHECKS

Contraband checks seek to identify objects that prohibited from entering a secure area. These checks often detect metals, weapons, or explosives. Contraband checks are casually thought to be detective controls, but their presence makes them a viable deterrent to actual threats.

MOTION DETECTORS AND OTHER PERIMETER ALARMS

Ultrasonic and *microwave motion detectors* work like Doppler radar used to predict the weather. A wave of energy is emitted, and the "echo" is returned when it bounces off an object. A motion detector that is 20 ft away from a wall will consistently receive an echo in the time it takes for the wave to hit the wall and bounce back to the receiver, for example. The echo will return more quickly when a new object, such as a person walking in range of the sensor, reflects the wave.

A *photoelectric motion sensor* sends a beam of light across a monitored space to a photoelectric sensor. The sensor alerts when the light beam is broken.

Ultrasonic, microwave, and infrared motion sensors are active sensors, which means they actively send energy. Consider a passive sensor as a read-only device; an example is a *passive infrared (PIR) sensor*, which detects infrared energy created by body heat.

DOORS AND WINDOWS

Always consider the relative strengths and weaknesses of doors, windows, walls, floors, ceilings, etc. All should be equally strong from a defensive standpoint, as attackers will target the weakest spot.

Egress must be unimpeded in case of emergency, so a simple push button or motion detectors are frequently used to allow egress. Outward-facing emergency doors should be marked for emergency use only and equipped with panic bars, which will trigger an alarm when used.

Glass windows are structurally weak and can be dangerous when shattered. Bullet-proof or explosive-resistant glass can be used for secured areas. Wire mesh or

security film can lower the danger of shattered glass and provide additional strength. Alternatives to glass windows include polycarbonate such as Lexan™ and acrylic such as Plexiglas®.

WALLS, FLOORS, AND CEILINGS

The walls around any internal secure perimeter, such as a data center, should start at the floor slab and run to the ceiling slab. These are called slab-to-slab walls. Raised floors and drop ceilings can obscure where the walls truly start and stop. An attacker should not be able to crawl under a wall that stops at the top of the raised floor, or climb over a wall that stops at the drop ceiling.

GUARDS

Guards are a dynamic control in a variety of situations. Guards can inspect access credentials, monitor CCTVs and environmental controls, respond to incidents, and act as a general deterrent. All things being equal, criminals are more likely to target an unguarded building over a guarded building.

Professional guards have attended advanced training and/or schooling; amateur guards have not. The term *pseudo guard* means an unarmed security guard.

DOGS

Dogs provide perimeter defense duties, particularly in controlled areas, such as between the exterior building wall and a perimeter fence. The primary drawback to using dogs as a perimeter control is the legal liability.

SITE SELECTION, DESIGN, AND CONFIGURATION

Selection, design, and configuration describes the process of building a secure facility like a data center starting from the site selection process and going through the final design.

SITE SELECTION ISSUES

A greenfield is an undeveloped lot of land, which is the design equivalent of a blank canvas. In a similar way, site selection is the greenfield process of choosing a site to construct a building or data center.

Utility reliability

The reliability of local utilities is a critical concern for site selection purposes. Electrical outages are among the most common of all failures and disasters. Uninterruptible power supply (UPS) will provide protection against electrical failure

for a short period (usually several hours or less). Generators provide longer protection but require refueling in order to operate for extended periods.

Crime

Local crime rates also factor into site selection. The primary issue is employee safety; all employees have the right to a safe working environment. Additional issues include theft of company assets.

SITE DESIGN AND CONFIGURATION ISSUES

Once the site has been selected, a number of design decisions must be made. Will the site be externally marked as a data center? Is there shared tenancy in the building? Where is the telecom demarcation point, or telecom *demark*?

Site marking

Many data centers are not externally marked in order to avoid drawing attention to the facility and its expensive contents. A modest building design might be an effective way to avoid attention.

Shared tenancy and adjacent buildings

Other tenants in a building can pose security issues, as they are already behind the physical security perimeter. A tenant's poor practices in visitor security can endanger your security.

Adjacent buildings pose a similar risk. Attackers can enter a less secure adjacent building and use that as a base to attack an adjacent building, often breaking in through a shared wall.

Shared demarc

A crucial issue to consider in a building with shared tenancy is a shared demarc, which is the demarcation point at which the Internet service provider (ISP) responsibility ends and the customer's begins. Most buildings have one demarc area where all external circuits enter the building. Access to the demarc allows attacks on the confidentiality, integrity, and availability of all circuits and the data flowing over them.

Media storage facilities

Offline storage of media for disaster recovery, potential legal proceedings, or other legal or regulatory purposes is commonplace. An off-site media storage facility will ensure that the data is accessible even after a physical disaster at the primary facility. The purpose of the media being stored offsite is to ensure continued access, which means the facility should be far enough removed from the primary facility to avoid the likelihood of a physical disaster affecting both the primary facility and the offsite storage location. Licensed and bonded couriers should transfer the media to and from the offsite storage facility.

SYSTEM DEFENSES

System defenses are one of the last lines of defense in a defense-in-depth strategy. These defenses assume that an attacker has physical access to the device or media containing sensitive information. In some cases, other controls may have failed and these controls are the final phase in data protection.

ASSET TRACKING

Detailed asset tracking databases enhance physical security. You cannot protect your data unless you know where and what it is. Detailed asset tracking databases support regulatory compliance by identifying where all regulated data is within a system. In case of employee termination, the asset database will show the exact equipment and data that the employee must return to the company. Data such as serial numbers and model numbers are useful in cases of loss due to theft or disaster.

PORT CONTROLS

Modern computers may contain multiple ports that may allow copying data to or from a system. Port controls are critical because large amounts of information can be placed on a device small enough to evade perimeter contraband checks. Ports can be physically disabled; examples include disabling ports on a system's motherboard, disconnecting internal wires that connect the port to the system, and physically obstructing the port itself.

ENVIRONMENTAL CONTROLS

Environmental controls provide a safe environment for personnel and equipment. Examples of environmental controls include power, HVAC, and fire safety.

ELECTRICITY

Reliable electricity is critical for any data center. It is one of the top priorities when selecting, building, and designing a site.

CRUNCH TIME

The following are common types of electrical faults:

- *Blackout*: prolonged loss of power
- *Brownout*: prolonged low voltage
- *Fault*: short loss of power
- *Surge*: prolonged high voltage
- *Spike*: temporary high voltage
- *Sag*: temporary low voltage

Surge protectors, UPS, and generators

Surge protectors protect equipment from damage due to electrical surges. They contain a circuit or fuse that is tripped during a power spike or surge, shorting the power or regulating it down to acceptable levels.

UPS provides temporary backup power in the event of a power outage. It may also "clean" the power, protecting against surges, spikes, and other forms of electrical faults.

Generators provide power longer than UPS and will run as long as fuel for the generator is available on site. Disaster recovery strategies should consider any negative impact on fuel supply and delivery.

EMI

Electricity generates magnetism, so any electrical conductor emits electromagnetic interference (EMI). This includes circuits, power cables, network cables, and many others. Network cables that are shielded poorly or are installed too closely together may suffer *crosstalk,* where magnetism from one cable crosses over to another nearby cable. This primarily affects the integrity of the network or voice data, but it might also affect the confidentiality.

Proper network cable management can mitigate crosstalk. Therefore, never route power cables close to network cables. The type of network cable used can also lower crosstalk. For example, *unshielded twisted pair* (UTP) cabling is far more susceptible than *shielded twisted pair* (STP) or *coaxial cable*. *Fiber optic cable* uses light instead of electricity to transmit data and is not susceptible to EMI.

HEATING, VENTILATION, AND AIR CONDITIONING

Heating, ventilation, and air conditioning (HVAC) controls keep the air at a reasonable temperature and humidity. They operate in a closed loop and recirculate treated air to help reduce dust and other airborne contaminants. HVAC units should employ positive pressure and drainage.

Data center HVAC units are designed to maintain optimum heat and humidity levels for computers. Humidity levels of 40–55% are recommended. A commonly recommended set point temperature range for a data center is 68–77 F (20–25°C).

Static and corrosion

The proper level of humidity can mitigate static by grounding all circuits in a proper manner and using antistatic sprays, wrist straps, and work surfaces. All personnel working with sensitive computer equipment such as boards, modules, or memory chips should ground themselves before performing any work.

High humidity levels can allow the water in the air to condense onto and into equipment, which may lead to corrosion. Maintaining proper humidity levels mitigates corrosion as well.

HEAT, FLAME, AND SMOKE DETECTORS

Heat detectors emit alerts when temperature exceeds an established safe baseline. They may trigger when a specific temperature is exceeded or when temperature changes at a specific rate (such as "10 F in less than 5 minutes").

Smoke detectors work through two primary methods: *ionization* and *photoelectric*. Ionization-based smoke detectors contain a small radioactive source that creates a small electric charge. Photoelectric sensors work in a similar fashion, except that they contain an LED (light-emitting diode) and a photoelectric sensor that generates a small charge while receiving light. Both types of alarms will sound when smoke interrupts the radioactivity or light by lowering or blocking the electric charge.

Flame detectors detect infrared or ultraviolet light emitted in fire. One drawback to this type of detection is that the detector usually requires line of sight to detect the flame; smoke detectors do not have this limitation.

PERSONNEL SAFETY, TRAINING, AND AWARENESS

Personnel safety is the primary goal of physical security. Safety training provides a skill set for personnel, such as learning to operate an emergency power system. Safety awareness can change user behavior in a positive manner. Both safety training and awareness are critical to ensure the success of a physical security program because you can never assume that personnel will know what to do and when to do it.

Evacuation routes

Post evacuation routes in a prominent location, as they are in hotel rooms, for example. Advise all personnel and visitors of the quickest evacuation route from their areas.

All sites should designate a meeting point, where all personnel will meet in the event of emergency. Meeting points are critical; tragedies have occurred when a person does not know another has already left the building and so he or she reenters the building for an attempted rescue.

Evacuation roles and procedures

The two primary evacuation roles are *safety warden* and *meeting point leader*. The safety warden ensures that all personnel safely evacuate the building in the event of an emergency or drill. The meeting point leader assures that all personnel are accounted for at the emergency meeting point. Personnel must follow emergency procedures, which includes following the posted evacuation route in case of emergency or drill.

Duress warning systems

Duress warning systems are designed to provide immediate alerts in the event of emergencies, such as severe weather, threat of violence, chemical contamination, etc. Duress systems may be local and include technologies such as use of overhead speakers or automated communications such as email or text messaging.

Travel safety

Personnel must be safe while working in all phases of business. This does not only refer to on-site work; it also includes authorized work from home and business travel. Telecommuters should have the proper equipment, including ergonomically safe workstations.

Business travel to certain areas can be dangerous. When organizations such as the US State Department Bureau of Consular Affairs issue travel warnings (http://travel.state.gov/), they should heeded by personnel before embarking on any travel to foreign countries.

ABCDK FIRES AND SUPPRESSION

The primary safety issue in case of fire is safe evacuation. Fire suppression systems extinguish fires, and different types of fires require different suppressive agents. These systems are typically designed with personnel safety as the primary concern.

Classes of fire and suppression agents

Class A fires are common combustibles such as wood and paper. This type of fire is the most common and should be extinguished with water or soda acid.

Class B fires are burning alcohol, oil, and other petroleum products such as gasoline. They are extinguished with gas or soda acid. You should never use water to extinguish a Class B fire.

Class C fires are electrical fires fed by electricity and may ignite in equipment or wiring. Electrical fires are conductive fires, and the extinguishing agent must be nonconductive, such as any type of gas. Many sources erroneously list soda acid as recommended for Class C fires, this is incorrect, as soda acid can conduct electricity.

Class D fires involve burning metals; use dry power to extinguish them.

Class K fires are kitchen fires, such as burning oil or grease. Extinguish class K fires with wet chemicals. Table 3.5 summarizes the classes of fire and suppression agents.

TYPES OF FIRE SUPPRESSION AGENTS

All fire suppression agents work via four possible methods, sometimes in combination: reducing the temperature of the fire, reducing the supply of oxygen, reducing the supply of fuel, and interfering with the chemical reaction within fire.

Water

Water suppresses fire by lowering the temperature below the *kindling point*, also called the *ignition point*. Water is the safest of all suppressive agents and therefore recommended for extinguishing common combustible fires such as burning paper or wood. It is important to cut electrical power when extinguishing a fire with water to reduce the risk of electrocution.

Table 3.5 Classes of Fire and Suppression Agents

US Class	Europe Class	Material	Suppression Agent
A	A	Ordinary combustibles such as wood and paper	Water or soda acid
B	B	Liquid	Halon/Halon substitute, CO_2, or soda acid
B	C	Flammable gases	Halon/Halon substitute, CO_2, or soda acid
C	E	Electrical equipment	Halon/Halon substitute, CO_2
D	D	Combustible metals	Dry powder
K	F	Kitchen (oil or fat) fires	Wet chemicals

Soda acid

Soda acid extinguishers are an older technology that use soda (sodium bicarbonate) mixed with water. There is a glass vial of acid suspended inside the extinguisher and an external lever breaks the vial. In addition to suppressing fire by lowering temperature, soda acid also has additional suppressive properties beyond plain water, as it creates foam that can float on the surface of some liquid fires, cutting off the oxygen supply.

Dry powder

Extinguishing a fire with dry powder, such as sodium chloride, works by lowering temperature and smothering the fire, starving it of oxygen. Dry powder is often used to extinguish metal fires. Flammable metals include sodium, magnesium, and many others.

Wet chemicals

Wet chemicals are primarily used to extinguish kitchen fires, which are Type K fires in the United States and Type F in Europe. However, wet chemicals may also be used on Type A (common combustible) fires. The chemical is usually potassium acetate mixed with water. This covers a grease or oil fire in a soapy film that lowers the temperature.

CO_2

Fires require oxygen as fuel, so removing oxygen smothers fires in CO_2 fire suppression. A major risk associated with CO_2 is that it is odorless and colorless, and our bodies will breathe it like air. By the time we begin suffocating due to lack of oxygen, it is often too late. This makes CO_2 a dangerous suppressive agent, so it is only recommended for use in unstaffed areas, such as electrical substations.

Halon and Halon substitutes

Halon extinguishes fire via a chemical reaction that consumes energy and lowers the temperature of the fire. However, Halon is currently being phased out in favor of replacements with similar properties.

Montreal accord

Halon has ozone-depleting properties. Because of this effect, the 1989 *Montreal Protocol* (formally called the *Montreal Protocol on Substances That Deplete the Ozone Layer*) banned production and consumption of new Halon in developed countries as of Jan. 1, 1994. However, existing Halon systems may be used, and while new Halon is not being produced, recycled Halon may be used.

FAST FACTS

Recommended replacements for Halon include the following systems:

- Argon
- FE-13
- FM-200
- Inergen

FE-13 is the newest of these agents, and comparatively safe. Breathing it in is safe in concentrations of up to 30%. Other Halon replacements are usually only safe for breathing up to a 10–15% concentration.

Sprinkler systems

Wet pipes have water right up to the sprinkler heads; therefore, the pipes are "wet." The sprinkler head contains a metal, which is common in older sprinklers, or small glass bulb designed to melt or break at a specific temperature. Once that occurs, the sprinkler head opens and water flows. Each head will open independently as the trigger temperature is exceeded.

Dry pipe systems also have closed sprinkler heads, but the difference is compressed air fills the pipes. A valve holds the water back and it will remain closed as long as sufficient air pressure remains in the pipes. As the dry pipe sprinkler heads open, the air pressure drops in each pipe, allowing the valve to open and send water to that head.

Deluge systems are similar to dry pipes, except the sprinkler heads are open and larger than dry pipe heads. The pipes are empty at normal air pressure; a deluge valve holds the water back. The valve opens when a fire alarm triggers.

Preaction systems are a combination of wet, dry, or deluge systems and require two separate triggers to release water. Single interlock systems release water into the pipes when a fire alarm triggers. The water releases once the head opens. Double interlock systems use compressed air, the same as dry pipes. However, the water will not fill the pipes until both the fire alarm triggers and the sprinkler head opens.

Portable fire extinguishers

All portable fire extinguishers should be marked with the type of fire they can extinguish. Portable extinguishers should be small enough so that any personnel who may need to use one can do so.

SUMMARY OF EXAM OBJECTIVES

In this large domain we began by describing fundamental logical hardware, operating systems, and software security components, as well as how to use those components to design, architect, and evaluate secure computer systems. Understanding these fundamental issues is critical for any information security professional.

We then moved on to cryptography, which dates to ancient times but is very much a part of our modern world, providing security for data in motion and at rest. Modern systems such as PKI put all the cryptographic pieces into play via the use of symmetric, asymmetric, and hash-based encryption to provide confidentiality, integrity, authentication, and nonrepudiation. You have learned how the pieces fit together; slower and weaker asymmetric ciphers such as RSA and Diffie-Hellman are used to exchange faster and stronger symmetric keys such as AES and DES. The symmetric keys are used as session keys to encrypt short-term sessions, such as web connections via HTTPS. Digital signatures employ public key encryption and hash algorithms such as MD5 and SHA-1 to provide nonrepudiation, authentication of the sender, and integrity of the message.

Finally, physical security is implicit in most other security controls, and it is often overlooked. We must always seek balance when implementing controls from all eight domains of knowledge. All assets should be protected by multiple defense-in-depth controls that span multiple domains. For example, a file server can be protected by policy, procedures, access control, patching, antivirus, OS hardening, locks, walls, HVAC, and fire suppression systems, among other controls). A thorough and accurate risk assessment should be conducted for all assets needing protection.

TOP FIVE TOUGHEST QUESTIONS

(1) Which of the following is true for digital signatures?
- **(A)** The sender encrypts the hash with a public key
- **(B)** The sender encrypts the hash with a private key
- **(C)** The sender encrypts the plaintext with a public key
- **(D)** The sender encrypts the plaintext with a private key

(2) Under which type of cloud service level would Linux hosting be offered?
- **(A)** IaaS
- **(B)** IDaaS
- **(C)** PaaS
- **(D)** SaaS

(3) A criminal deduces that an organization is holding an offsite meeting and there are few people in the building, based on the low traffic volume to and from the parking lot. The criminal uses the opportunity to break into the building to steal laptops. What type of attack has been launched?
- **(A)** Aggregation
- **(B)** Emanations
- **(C)** Inference
- **(D)** Maintenance Hook

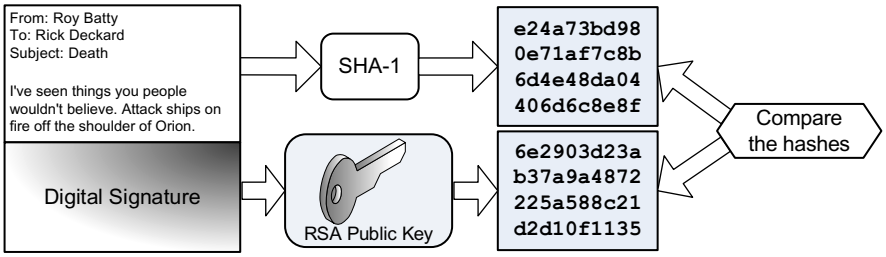

FIG. 3.5

Hotspot.

(4) EMI issues such as crosstalk primarily impact which aspect of security?
- **(A)** Confidentiality
- **(B)** Integrity
- **(C)** Availability
- **(D)** Authentication

(5) Hotspot: You receive the following signed email from Roy Batty. You determine that the email is not authentic, or it has changed since it was sent. Click on the locally generated message digest that proves the email lacks nonrepudiation (Fig. 3.5).

ANSWERS

1. *Correct Answer and Explanation*: B. The sender generates a hash of the plaintext and encrypts the hash with a private key. The recipient decrypts the hash with a public key.
   Incorrect Answers and Explanations: Answers A, C, and D are incorrect. The sender encrypts the hash with the private key, not public. The plaintext is hashed, and not encrypted.
2. *Correct Answer and Explanation*: A. Answer A is correct; IaaS (infrastructure as a service) provides an entire virtualized operating system, which the customer configures from the OS on up.
   Incorrect Answers and Explanations: Answers B, C, and D are incorrect. IDaaS (identity as a service) is also called cloud identity. IDaaS allows organizations to leverage cloud service for identity management. PaaS (platform as a service) provides a preconfigured operating system, and the customer configures the applications. SaaS (software as a service) is completely configured from the operating system to applications, and the customer simply uses the application.
3. *Correct Answer and Explanation*: C. Inference requires an attacker to "fill in the blanks" and deduce sensitive information from public information.
   Incorrect Answers and Explanations: Answers A, B, and D are incorrect. Aggregation is a mathematical operation where all questions are asked and

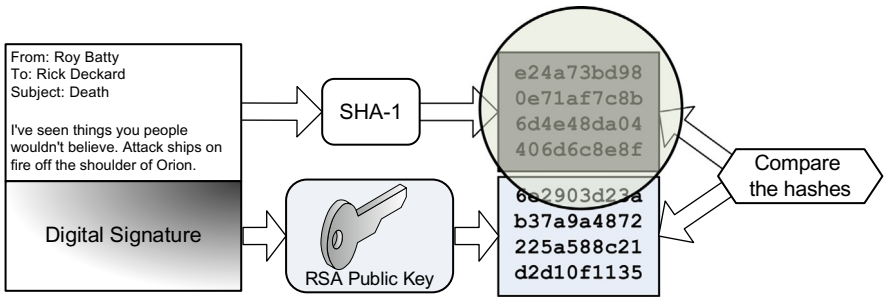

FIG. 3.6

Hotspot answer.

all answers are received; there is no deduction required. Emanations are energy broadcast from electronic equipment. Maintenance hooks are system maintenance backdoors left by vendors.

4. *Correct Answer and Explanation*: B. While EMI issues like crosstalk could impact all aspects listed, it most commonly impacts integrity.
   Incorrect Answers and Explanations: Answers A, C, and D are incorrect; confidentiality can be impacted (such as hearing another conversation on a voice phone call). In extreme cases, availability and authentication could be impacted, such as where crosstalk is so severe as to stop systems from functioning. These scenarios are far less common than simple integrity violation caused by EMI issues, such as crosstalk (Fig. 3.6).

ENDNOTES

1. *Three minutes with security expert Bruce Schneier*. https://www.schneier.com/news/archives/2001/09/three_minutes_with_s.html [accessed 29.04.16].
2. Schneier B. *Applied cryptography*. New York, NY: Wiley; 1996.
3. Scott R. *Bladerunner*. Warner Bros; 1982.